CLAIMS

We claim:

1 A method for preventing unauthorized use of digital content data to be transferred from a first system to a second system comprising:

locating an archive of a digital content data at the first system;

determining transaction data of the second system;

determining whether the transaction data of the second system indicates whether the second system is a valid recipient of the archive; and

transferring the archive from the first system to the second system if the second system is a valid recipient.

2 The method of claim 1 further comprising, if the second system is not a valid recipient, transferring the archive from the first system to the second system, the operation of the archive failing in the second system.

3 The method of claim 1 wherein the first system comprises a hard media and wherein the second system comprises a computer system.

4 The method of claim 1 wherein the first system comprises a first computer system and wherein the second system comprises a second computer system.

5 The method of claim 4 wherein the first and second computer systems are remotely located.

6 The method of claim 1 wherein determining transaction data of the second system comprises determining a data element selected from the group of data elements consisting of: transaction identification; system configuration information; manufacturer, serial number, and physical properties.

7 The method of claim 1 wherein determining transaction data of the second system comprises downloading an analysis tool to the second system, and running the analysis tool to examine the second system and to generate a unique identifying value that identifies the second system as the transaction data.

8 The method of claim 7 wherein the unique identifying value is deposited in the archive that is transferred to the second system.

9 The method of claim 8 wherein the unique identifying value is encrypted and interleaved with the digital content data in the transferred archive.

10 The method of claim 1 further comprising modifying the archive with the transaction data before transferring the archive.

11 The method of claim 10 further comprising increasing a memory allocation of the archive before modifying the archive with the transaction data.

12 The method of claim 11 further comprising creating a map of the increased memory allocation.

13. The method of claim 12 further comprising storing the map in the archive, or in memory locations of the second system, or in the first system..

14 The method of claim 1 further comprising, before transferring the archive, removing a plurality of original data segments from memory locations of the archive and storing false data at the memory locations.

15 The method of claim 14 further comprising storing the original data in the archive, or in memory locations of the second system, or in the first system.

16. The method of claim 15 further comprising generating a map of the memory locations.

17 The method of claim 16 further comprising storing the map in the archive, or in memory locations of the second system, or in the first system.

18 The method of claim 14 wherein the false data comprises a machine instruction that initiates an abnormal condition in the digital content data when processed.

19 The method of claim 14 wherein the second system, following transfer of the archive, replaces the false data with the original data segments if the second system is a valid recipient.

20 The method of claim 19 wherein the second system replaces the false data by the original data segments immediately prior to execution of the corresponding memory locations, and replaces the original data by the false data immediately following execution of the corresponding memory locations.

21 A method for preventing unauthorized use of digital content data hosted on a system comprising:

examining system devices that are operating in the system;

determining whether any of the system devices are emulator devices; and

initiating a defense action, in event that an emulator device is operating on the system.

22 The method of claim 21 wherein the system devices comprise physical devices or logical entities.

23 The method of claim 21 wherein the emulator devices comprise hardware-based emulator devices or software-based emulator devices.

24 A method for preventing unauthorized use of digital content data hosted on a system comprising:

determining whether an unauthorized use of the digital content data is in progress; and

in the case where an unauthorized use is determined, initiating a defense action by disabling an input device.

25 The method of claim 24 wherein disabling an input device comprises disabling a combination of keystrokes at a keyboard input device.

26 The method of claim 24 further comprising disabling the input device with regard to user interface windows related to the unauthorized use.

27 The method of claim 26 wherein the input device comprises a keyboard or a mouse.

28 A method for preventing unauthorized use of digital content data hosted on a system comprising:

executing a plurality of system processes;

monitoring at each process for unauthorized use and each process transferring a status message to another process related to the unauthorized use; and

each process determining whether an unauthorized use has occurred, and, if such a determination is made, initiating a defense action.

29 The method of claim 28 wherein the status messages further relate to authorized use.

30 The method of claim 28 further comprising interleaving and encrypting each status message before transferring the status message.

31 The method of claim 28 wherein the status messages are temporarily stored at a virtual memory location on the system.

32 A method for preventing unauthorized use of digital content data hosted on a system comprising:

during the operation of a function operating on the system, determining whether an unauthorized use of the digital content data is in progress; and

in the case where an unauthorized use is determined, initiating a defense action that is integrated into the function.

33 The method of claim 32 wherein the function is a non-defensive function.

34 The method of claim 32 wherein the defense action comprises reading and writing data values critical to system operation repeatedly to a decoy process.